МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЛАБОРАТОРНА РОБОТА №2

З дисципліни «Криптографія»

Варіант 1

Виконали:
студенти 3 курсу ФТІ
групи ФБ-93
Абдуллаєва Есміра
Шовак Мирослав

Викладач:
Селюх П. В.

м.Київ – 2021

Мета роботи: засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.

Завдання

1. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
2. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
3. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
4. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Хід роботи та опис труднощів

Основу для роботи з текстовими файлами ми взяли з попередньої лабораторної роботи. Ми покроково виконували наші завдання . Текстом для шифрування була обрана пісня , отже ми так як і раніше відформатували текст за допомогою regular expression , та replace , крім того додали до нашого алфавіту букву "ъ". Ми створили функцію , яка генерує випадкові ключі в залежності від вказаної довжини, потім ми створили функції для шифрування і розшифрування тексту . Ознайомившись з шифром Віженера , були застосовані формули для знаходження значення зашифрованої і розшифрованої букви. У функціях шифрування і розшифрування , ми працювали безпосередньо з індексами букв нашого алфавіту. Для пошуку зашифрованої букви , у відповідність кожній букві ВТ ставилася буква нашого ключа , обчислювали ми значення відповідної букви ключа за допомогою `keyindexes[i % len(keyindexes)]` , де keyindexes -масив значень букв ключа , і це порядок букви в тексті , і беремо це по модулю довжини ключа. Вся формула обчислення зашифрованої букви `EncodLeter=(keyindexes[i%len(keyindexes)]+alphabet.index(text[i]))%len(alphabet)`.Для розшифрування букви використовується формула `DecodLeter=(alphabet.index(text[i])-keyindexes[i%len(keyindexes)]+len(alphabet))%len(alphabet)`. Усі букви заносяться у масив і в результаті ми просто виводимо масив і отримуємо потрібний нам текст. Наступною проблемою для нас було те , що ми не дуже знали як розбити текст на блоки , але потім ми дізналися про таку властивість роботи з текстом і написали цикл , який розбиває текст на блоки в залежності від довжини ключа

```
for i in range(size):
       blocks.append(text[i::size]).
```

Підготувавши усі потрібні функції ми знайшли спочатку індекс відповідності для наших блоків і дійшли висновку , що найбільш наближене значення до індексу відповідності нашого тексту це значення блоку де ключ довжини 12. Звідси висновок , що скоріше за все довжина нашого ключа = 12 . Підставивши значення нашого ШТ , довжини ключа і найчастішої букви мови , ми отримали ключ вшебспирбуря. Інтуїтивно стало зрозуміло , що мається на увазі В.Шекспір "Буря". Поміняли букву 'б' на 'к' і отримали наш ключ , після чого розшифрували ШТ.

Код програми

```
import re
import random

file = open("result.txt", "w") # result
decode

file1 = open("1.txt", "r").read()
text1 = re.sub(r"[^а-яё]+", "",
file1.lower()).replace("ё","е").replace("
", "") # encoding

file2 = open("2.txt", "r")
text2 = file2.read() # decoding

alphabet =
['а','б','в','г','д','е','ж','з','и','й','к
','л','м','н','о','п','р','с','т','у','ф','
х','ц','ч','ш','щ','ъ','ы','ь','э','ю','я']

def rand_key():
    mass = []
    print('Enter length of key:')
    long = int(input())
    j = 0
    while j < long:
        i =
alphabet[random.randint(0,len(alphabet)-1)]
        mass.append(i)
        j+=1
    key = ''.join(mass)
    print('key:', key)
    return key

def encrypt (text, key):
    keyindexes = []
    ciphertext = []
    for i in range(len(key)):
        keyindexes.append(
alphabet.index(key[i]) )

    for i in range(len(text)):
        EncodLeter = ( keyindexes[i %
len(keyindexes)] + alphabet.index(text[i])
) % len(alphabet)

ciphertext.append(alphabet[EncodLeter])

    cipheredtext = ''.join(ciphertext)
    return cipheredtext

def decrypt (text, key):
    keyindexes = []
    entrancetext = []
    for i in range(len(key)):
        keyindexes.append(
alphabet.index(key[i]) )

    for i in range(len(text)):
        DecodLeter = (
alphabet.index(text[i]) - keyindexes[i %
len(keyindexes)] + len(alphabet) ) %
len(alphabet)

entrancetext.append(alphabet[DecodLeter])

    entrancedtext = ''.join(entrancetext)
    return entrancedtext

def compliance index(text):
    arr = []
    for i in alphabet:
        letter = text.count(i)
        arr.append(letter * (letter-1))

    I = sum(arr) / (len(text)*(len(text)-
1))
    return I

def ComplianceIndexForDecrypt(text, size):
    blocks = []
    index = []
    for i in range(size):
        blocks.append(text[i::size])
    for i in range(len(blocks)):

index.append(compliance index(blocks[i]))
    print("Len of key:", size, ",",
"Comliance index for block:",
sum(index)/len(blocks))
    return blocks

def MaxLetter(text):
    letter = []
    for i in alphabet:
        letter.append(text.count(i))
    return letter.index(max(letter))

def MakeKey (text, size, letter):
    keys = []
    blocks =
ComplianceIndexForDecrypt(text, size)
    for i in range(len(blocks)):
        maxcount = MaxLetter(blocks[i])
        key = (maxcount -
alphabet.index(letter)) % len(alphabet)
        keys.append(alphabet[key])
    key = ''.join(keys)
    return key

# main part

#task1
key1 = rand_key()
en = encrypt(text1, key1)
print("Encrypted text:" , en)
print("Decrypted text:", decrypt(en, key1))
print("Comliance index:",
compliance_index(en),'\n')

#task2
for r in range(1,len(alphabet)):
    ComplianceIndexForDecrypt(text2, r)

print('\n')
print('Make key:', MakeKey(text2, 12, 'о'))
key = 'вшекспирбуря'
print('Key:', key)
decode = decrypt(text2, key)
print("Decrypted text:", decode)
file.write(decode)
```

Результат роботи

```
Enter length of key:
2
key: хю
Encrypted text: дмцйъвгчцэгажжрсэгивюьюеюжрхьзнемьоххвмюагвгзиагврлървжжкъозжвщлхэдогчхьжъкргягзшмепзъзгдйхнглагцмабгзьжбщцмвгжгбнфрскэлирцмиреюцмыжчгблхцькгоъаэлрнгбамоюъ
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.04786515852089623

Enter length of key:
3
key: юфь
Encrypted text: нвэйцалщюцьбйьнррымюйюыьоюрфъргммымюлймэюмшкэзюмшчлцольнкщмрьйжшйюуловхютнъеомхкзчкоеоъжбняьнвнйцамяямэгжачввйгебгкгыррижбпршксжмюшкдьюгайюмбквмгцдплпмчэмньг
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.03736927917255786

Enter length of key:
4
key: еиси
Encrypted text: фцтукмюнзащррвъбзятттшихивъежгчхцшшеяюцокямусдкуммхкъюрцфцшчрюрйхсзфшябежвдцьяйусфцхцгдчнауечящрнхцрлясмрзгйцюнцнэчдьнфнхдьйцдъхихцлрунсхсакфяшккцхачялрцкик
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.04324773587068669

Enter length of key:
5
key: йзгыч
Encrypted text: шхджьнфизпсмогиыгвйбцзкыэйшхъхыцуйющзъиетйсяетъейыдфиндсшпазыпргыцзвкэчагщиешхйшчржйзъщяныштгкеътияефксдюсуюяецмфагшжхчгсфцнычъхлчнхйгщоурыпоусльлпрщжчкойрйм
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.03533761320646567

Enter length of key:
10
key: бвкщцжкъшт
Encrypted text: ррзбыкуяькйзсюэшвщжьювнцюхчмшрусцдэцмсеакдфъдпщьжцьплигочжзвукуюъужщзвпыжфзавчмжуплйджчшцкчрнжедчсяьамефяэотхьаозчывхемфкйпщиьфцмитермюшлтзшкюфжыиозубпесдпюл
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.034274013782210504

Enter length of key:
11
key: тъодбъэчски
Encrypted text: биппжюфьуврчецхуцжеычищъюдтмэхгщшабюдшзхаушагбжпювдцьхъпъйсмпдщохтцэфпузхвжщдипткэхэвьддяэпбйхиыпмаесткблгмоцяяйнйжйнцрянаипнцзсоцшврйнзэпццщвярмохцефхцлъу
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.033175385634402026

Enter length of key:
12
key: овяфдсьаалия
Encrypted text: эраяйхйевгрдшкрмаркклпяюврждпопрщппощмнукдофыбыжъбйгйисчнпакмыиюьяпыцшоарррхгкбофлнюусрцщллаъцрцэгвпфкйзуфътрмщхципяэдлцптжияптрлмнфкбщрюышечцпудзбяакглщбяу
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.033875960105468304

Enter length of key:
13
key: ржолуувичхиос
Encrypted text: яфпщичпнщнрушчазтбмхчьиюсбшойевтцюеиеююпрцчблыщгмйюхшыдяэшйэхцхэжнъгбыиржждягюэьфцбтщйсъуаыкэщдюзмеальъчюъжчбпниъфэрввъуажфмеиъюсффуухшохчннъяалруаосцъацзсх
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.0335798081699721

Enter length of key:
14
key: рдхцйпиижщтитыф
Encrypted text: ятцбоуклыкрчжьбцсхчщхжатштмкрвзецэпщщйхадцюигяьсцкфяндиьбръжычхоэяиискдюэхфьлшшзуцыювахзтыфчсцбцгжщфтащчшпоенмаищбйбеибдтбяыдявгцецнэоочфяымкргжосруфбцжквйдъ
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.03246525787589394

Enter length of key:
15
key: втдчбмэддюиуерю
Encrypted text: саевжрфйжцршршпфогелцзлдоидчрьфбфеиьзысмсхуфмлежеезфйцлрдсхофъсяецзгуоцмеопюгцевьрзтощебвгсэдкпэтймуцуцекюяыпцмхйкчтчмккячйеъуцфюмблшазюсчщсутфгкытлнрхпеъмм
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.03284102054593858

Enter length of key:
16
key: аньофцймнэзпипим
Encrypted text: пыэщцъцспхпфучщюьмкшбцрмэзшбинъырыгюфнцъцяхущыоосчыцицфюймяъчхфдъьнгжченышлщбцноцяьдзыиявцъиюцэлтаъяыцчхфеукмэхсстиэуиешхкъбмэыюрнаъъюлсцкззныцьепдыпечпшлапн
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.03475804705312902

Enter length of key:
17
key: оювампкуъпкъыдцпю
Encrypted text: эмглсучыьэтядмкбънммммцкгъаьъчцияямховчцэухиушгмжзущыгфнфацшкбтзбижпээорцмныплбшызньэоярютсюхуйэыекюизъбьэйишкобзфыяеушбъъжпуюушжмякюзкбсгълвшсышгястэфуэтйьчве
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.03261174162813507

Enter length of key:
18
key: вжсхнесмгыбохафглж
Encrypted text: сфтатйюсеуйуаиехзеррюхфебмфнбмзлдстцвэюгцзярсдфргдпрршповбтхгфргеыхягущявдвсючянсддьесжяэлссздыцьсэймсгйылчбжфюъюкзывнзъэнэхпфхшбхсучфеаныхшщпщзищвифяпойъоъ
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.032911077993045205

Enter length of key:
19
key: аопиючъвгпйфннгсне
Encrypted text: пьрунвдядычоякхнмукыппиочлгчныгэыкбнънышкцвегхеэнпътхюхцмуяърляюпгошдыкгпюбсаэйцзъитфбежтъосьусщфмцйъилкчхпсырцюкмэоъдкяэххучзяэгхылирффхюпяосяоцхъюаыильиин
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.03336326696982435

Enter length of key:
20
key: зеупыктывчрькфбирчяз
Encrypted text: цуфъакяадпшбхьтъмцнсфеъплжгнвхвлъвишромхрзбуйпезрылйпжорбгдчщначяутъсэюхкттдбйнихоцэлчдчфьяэкгпщыьгхтибшвюцкезбыщнчпйыуптжбяфентчфкрьгньдяямсбяаиъиэжюяхвъих
Decrypted text: побледневшиелистьяокназарастаютпрозрачнойводойуводынетнисмертинидная прощаюсьстобойгорстьтеплапоследолгойзимыдонесемпятьминутдоутрадоживемнашеморевинып оглощае
Comliance index: 0.0317678678334416 06
```

Compliance index for our decrypted text	
Key lenght	Compliance index
2	0.04786515852089623
3	0.0373692791725578
4	0.04324773587068669
5	0.03533761320646567
10	0.034274013782210504
11	0.033175385634402026
12	0.033875960105468304
13	0.0335798081699721
14	0.03246525787509394
15	0.03284102054593858
16	0.03475804705312902
17	0.03261174162813507
18	0.032911077993045205
19	0.03336326696982435
20	0.031767867833441606

Compliance index for text in variant one:

```
Len of key: 1 , Compliance index for block: 0.032821177802678465
Len of key: 2 , Compliance index for block: 0.03432921421542369
Len of key: 3 , Compliance index for block: 0.03734839112182639
Len of key: 4 , Compliance index for block: 0.03846786795894798
Len of key: 5 , Compliance index for block: 0.032753684507439526
Len of key: 6 , Compliance index for block: 0.04242249836150345
Len of key: 7 , Compliance index for block: 0.032845671625834745
Len of key: 8 , Compliance index for block: 0.038394305262087654
Len of key: 9 , Compliance index for block: 0.037406913486166676
Len of key: 10 , Compliance index for block: 0.034343106655826135
Len of key: 11 , Compliance index for block: 0.03282596004503103
Len of key: 12 , Compliance index for block: 0.05436955673586635
Len of key: 13 , Compliance index for block: 0.032807635112857336
Len of key: 14 , Compliance index for block: 0.034253133094361496
Len of key: 15 , Compliance index for block: 0.03741441107403287
Len of key: 16 , Compliance index for block: 0.03846816039387033
Len of key: 17 , Compliance index for block: 0.0326076877752591
Len of key: 18 , Compliance index for block: 0.042619239781400246
Len of key: 19 , Compliance index for block: 0.03299852287693898
Len of key: 20 , Compliance index for block: 0.03839407833306634
Len of key: 21 , Compliance index for block: 0.03734596917614833
Len of key: 22 , Compliance index for block: 0.03436346417856434
Len of key: 23 , Compliance index for block: 0.03248823743567128
Len of key: 24 , Compliance index for block: 0.05435416649918132
Len of key: 25 , Compliance index for block: 0.032517536103743
Len of key: 26 , Compliance index for block: 0.03434857665414954
Len of key: 27 , Compliance index for block: 0.03762500312229972
Len of key: 28 , Compliance index for block: 0.0383860390427654
Len of key: 29 , Compliance index for block: 0.033132183908045974
Len of key: 30 , Compliance index for block: 0.04250450051229374
Len of key: 31 , Compliance index for block: 0.03270427461964246
```

Пошук ключа для зашифрованого тексту та розшифровка:

```
Len of key: 12 , Compliance index for block: 0.05436955673586635
Make key: вшебспирбуря
Key: вшекспирбуря
Decrypted text: действующиелицаалонзокорольнеаполитанскийсебастьянегобратпросперозаконный
```

Висновок: під час лабораторної роботи ми засвоїли методи частотного аналізу та здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.